SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set for at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosure generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.

TYPE OF REQUEST TYPE ☒--INITIAL ☐--Modification ☐--Deletion	DATE

PART I (To be completed by User)

1. NAME (LAST, First, MI)		2. SOCIAL SECURITY NUMBER
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. ACCOUNT CODE
6. JOB TITLE/FUNCTION	7. GRADE/RANK	8. PHONE (DSN if applicable)

STATEMENT OF ACCOUNTABILITY

I understand my obligations to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized access.

USER SIGNATURE	DATE

PART II (To be completed by User's Security Manager)

9. CLEARANCE LEVEL	10. TYPE OF INVESTIGATION	11. DATE OF INVESTIGATION
12 VERIFIED BY (Signature)	13. PHONE NUMBER	14. DATE

PART III (To be completed by User's Supervisor)

15. ACCESS REQUIRED (Location) – i.e. DMC or DMC's

16. ACCESS TO CLASSIFIED REQUIRED? ☒--NO ☐--YES	17. TYPE OF USER ☒--FUNCTIONAL ☐--SYSTEM ☐--SECURITY ADMINISTRATOR ☐--APPLICATION DEVELOPER ☐--OTHER (specify)

18. JUSTIFICATION FOR ACCESS

VERIFICATION OF NEED TO KNOW

I certify that this user requires access as requested in the performance of his/her job function.

19. SIGNATURE OF SUPERVISOR	20. ORG./DEPT.	21. PHONE NUMBER	22. DATE
23. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR	24. ORG./DEPT.	25. PHONE NUMBER	26. DATE

PART IV (To be completed by AIS Security Staff adding user)

27. USERID (Mainframe)	28. USERID (Mid-Tier)	29. USERID (Network)
30. SIGNATURE	31. PHONE NUMBER	32. DATE

INSTRUCTIONS

A Part I The following information is provided by the user when establishing or modifying their USERID

(1) NAME The last name, first name, and middle initial of the user
(2) SOCIAL SECURITY NUMBER The social security number of the user
(3) ORGANIZATION The user's current organization (i e , *DMC San Antonio)*
(4) OFFICE SYMBOL/DEPARTMENT The office symbol within the current organization (i e , *WEA32*)
(5) ACCOUNT CODE Account code, if required
(6) JOB TITLE/FUNCTION The job function (i e , *Systems Analyst, Pay Clerk, etc)*
(7) GRADE/RANK The civilian pay grade, military rank or CONT if contractor
(8) PHONE (DSN) The Defense Switching Network (DSN) phone number of the user If DSN is unavailable, indicate commercial phone number

USER'S SIGNATURE User must sign the SAAR form with the understanding that they are responsible an accountable for their password and access to the system(s)

B PART II The following information is provided by the User's Security Manager

(9) CLEARANCE LEVEL The user's current security clearance level and ADP Level (i e , *Secret, Top Secret, ADP I, ADP II, etc)*
(10) TYPE OF INVESTIGATION The user's last type of background investigation (i e , *NAC, NACI, or SSBI)*
(11) DATE OF INVESTIGATION The date of the last background investigation
(12) SIGNATURE The Security Manager or his representative signature indicates that the above clearance and investigation information has been verified Refer to Part V, # 34 e
(13) PHONE NBR The Security Manager's phone number
(14) DATE The date that the form was signed by the Security Manager or his representative

C PART III The following information is provided by the user's supervisor

(15) ACCESS REQUIRED *(Location)* The full name of the location at which access is required.
(16) ACCESS TO CLASSIFIED REQUIRED? Place an "X" in the appropriate box
(17) TYPE OF USER Place an "X" in the appropriate box
(18) JUSTIFICATION FOR ACCESS A brief statement to justify establishment of an initial USERID Provide appropriate information if the USERID or access to the current USERID is to be modified
(19) SIGNATURE OF SUPERVISOR The user's supervisor must sign the SAAR form to certify the user is authorized access to perform his/her job function Refer to Part V, # 34 c
(20) ORG/DEPT Supervisor's organization and department
(21) PHONE NUMBER Supervisor's phone number
(22) DATE The date the supervisor signs the SAAR
(23) SIGNATURE OF FUNCTIONAL DATA OWNER/OPR Signature of the functional appointee responsible for approving access to the system being requested Refer to Part V, # 34 d
(24) ORG /DEPT Functional appointee's organization and department
(25) PHONE NUMBER Functional appointee's phone number
(26) DATE The date the Functional appointee signs the SAAR

D PART IV The following information is provided by the AIS Security Staff who adds the user to the system.

*(27) USERID *(Mainframe)* User's Mainframe USERID (if applicable) To be filled out by user if already established
(28) USERID *(Mid-Tier)* User's Mid-Tier USERID (if applicable)
(29) USERID *(Network)* User's Network USERID (if applicable)
(30) SIGNATURE Signature of the Information Systems Security Officer (ISSO) or his representative
(31) PHONE NUMBER (DSN) The ISSO's DSN phone number
(32) DATE The date the ISSO signs the SAAR

E PART V This information is site specific and can be customized by either the DMC, functional activity, or the customer with approval of the DMC This information will specifically identify the access required by the user

(33) ACCESS REQUIRED Specify all resources to which access is required and the type access required, i e , read-only, write
(34) OPTIONAL USE This section is intended to add site specific information, as required

F DISPOSITION OF FORM

TRANSMISSION Form may be electronically transmitted, faxed, or mailed Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be handled as such

FILING Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DMC or by the Customer's ISSO Recommend file be maintained by ISSO adding the user to the system.

TANDEM /BURROUGHS SYSTEM

PART V **PLEASE INDICATE ACCESS REQUIREMENTS (SYSTEMS/APPLICATION)**

TANDEM GROUP NAME/USERID ________ . ________	**TRANSACTION CLASS** ______ **PROGRAM CLASS** ______ **BOFI** ______	**BURROUGHS ACCESS/PASSTHRU** **BURROUGHS USERID:** ______________
PS MAIL ACCESS **YES/NO**	**TAPS ID** **YES/NO**	**BURROUGHS TRANSACTION CLASSES:**
		___ ___

PART VI **ADDITIONAL INFORMATION**

____

____

____

____

____

PART V (To be completed by User)
(DISA or customer with DISA approval may customize Part V)

33. ACCESS REQUESTED (Site specific system or application information)

a) System(s)

b) Server(s)

c) Application(s)

d) Directory(s)

e) File(s)

f) Dataset(s)

34. OPTIONAL USE